REMARKS

Claims 1-32, 34-46, and 49-73 are pending. Claims 1-32, 34-46, and 49-62 are rejected under 35 U.S.C. § 112. Claims 1-4, 6-8, 12, 14-16, 21, 22, 26, 31, 32, 34, 39, 44, 45, 49-50, 53, 55-57, 62, 65, 66 and 69 are rejected under 35 U.S.C. § 102. Claims 5, 9, 10, 11, 13, 17-20, 23-25, 27-31, 33-38, 40-46, 50-54, 56-64, and 66-73 are rejected under 35 U.S.C. § 103. Applicant respectfully traverses these rejections. Claims 1, 22, 32, and 45 are herein amended. No new matter has been added.

Claim Rejections - 35 U.S.C. § 112

Claims 1-32, 34-46, and 49-62 are rejected under 35 U.S.C. § 112 as being indefinite. Specifically, it is asserted that independent claims 1, 22, 32, and 45, are indefinite because applying a key without access to a key is indefinite.

Independent claims 1, 22, 32, and 45 are amended to more clearly indicate that the cryptographic key is not accessed by the computer program. Claim 1 is amended to recite in part "a computer program ... that can compute results of using a cryptographic algorithm to apply a cryptographic key ... wherein said computer program does not access said cryptographic key." Claim 22 is amended to recite in part "performing a first set of actions which compute results of applying said cryptographic key to said data, said first set of actions not accessing, for their performance, said cryptographic key." Claim 32 is amended to recite in part "said action comprises computing results of applying a cryptographic key to first data; and said cryptographic key is not accessed in performance of said action." And, claim 45 is amended to recite in part "said first action comprises computing results of applying a cryptographic key to first data; and said cryptographic key is not accessed in performance of said first action." Accordingly, it is requested that the rejection, under 35 U.S.C. § 112, of independent claims 1, 22, 32, and 45 and their respective dependent claims, 2-21; 23-31; 34-44; and 46, 49-62, be reconsidered and withdrawn.

Claim Rejections - 35 U.S.C. § 102

Claims 1-4, 6-8, 12, 14-16, 21, 22, 26, 31, 32, 34, 39, 44, 45, 49-50, 53, 55-57, 62, 65, 66, and 69 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,643,775, issued to Granger *et al.* ("Granger *et al.*"). In support of the forgoing rejections, it is asserted, *inter alia*, in the instant Office Action that "[a]lthough Granger teaches that the encryption layer uses a key, Granger states in Col 7 lines 7-20, that the encryption layer code which performs the encryption and decryption of userdata may be written in a pseudocode, thus creating a new program that does not require said key."

Applicant respectfully disagrees with the premise that writing the encryption layer code in pseudocode creates a new program that does not require the key. As taught in Granger *et al.*, a key is used to encrypt and decrypt, and writing the encryption layer in pseudocode does not negate the use of the key. Writing the encryption layer in pseudocode "serves the purpose of concealing the implementation details of the Encryption Layer from pirates." (Column 6, lines 53-56). Writing the encryption layer in pseudocode merely implies writing the encryption layer in a different language. Preferably, as taught by Granger *et al.*, the language is difficult for pirates to evaluate. "The pseudocode is preferably written in a language of a non-existent machine or microprocessor, so that pirates cannot use commercially-available software development tools to disassemble and evaluate such copy protection functions." (Column 7, lines 1-7). Granger *et al.* does not teach, however, that writing the encryption layer in pseudocode provides a means for encrypting and decrypting without the use of the key.

All teachings in Granger *et al.* are directed to using a key for encryption and decryption, and nowhere does Granger *et al.* teach performing encryption or decryption without using a key. This is exemplified in FIG. 1A and FIG. 1B of Granger *el al.*, reproduced herein. As can be seen in FIG. 1A and FIG. 1B, a key is always provided to the

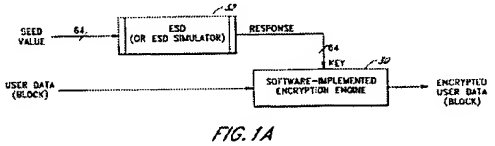


FIG. 1A

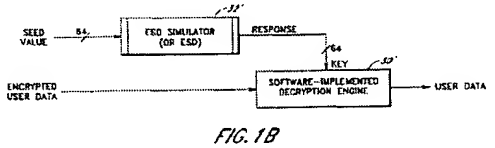


FIG. 1B

encryption engine 30 and to the decryption engine 30', regardless of the language used to implement the encryption layer.

Granger *et al.*, teaches that key-based encryption and decryption algorithms are used, and even provides examples of such algorithms. "The encryption engine 30 applies a key-based encryption algorithm to the block of user data. Any of a variety of encryption algorithms can be used for this purpose, including, for example, DES, RSA, or an exclusive-OR (XOR) algorithm." (Emphasis added) (Column 10, lines 21-25). "The decryption engine 30' implements a decryption algorithm which is the inverse of the algorithm used to encrypt the user data. Because the same seed value is used to generate the decryption key, the decryption key is the same as the encryption key ..." (Emphasis added) (Column 10, lines 56-61).

It is also implied, in the instant Office Action, that Granger *et al.*'s teaching of obfuscation at Column 9, lines 25-47, negates the use of a key. Again, Applicant respectfully disagrees. Obfuscation, as taught in Granger *et al.* "involves the use of a special development tool to translate selected blocks of the copy-protection code into much larger, less efficient blocks of code, so that the pirate has to disassemble and analyze significantly greater amounts of machine code to extract the function(s) or algorithm(s) performed by such code." (Column 7, line 63- Column, line 2). Thus, obfuscation, as taught in Granger *et al.*, merely reorganizes the code to make the code harder to analyze by pirates. Granger *et al.* does not teach that encryption and decryption do not require a key due to obfuscation.

Because Granger *et al.*, neither discloses nor suggests a computer program that can compute results of using a cryptographic algorithm to apply a cryptographic key wherein the computer program does not access the cryptographic key, it is requested that the rejection of claims 1-4, 6-8, 12, 14-16, 21, 22, 26, 31, 32, 34, 39, 44, 45, 49-50, 53, 55-57, 62, 65, 66, and 69, under 35 U.S.C. § 102 be reconsidered and withdrawn.

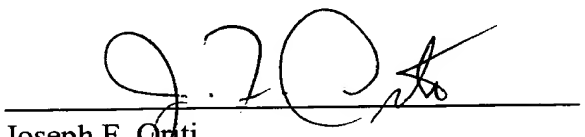
Claim Rejections - 35 U.S.C. § 103

Claims 5, 9, 10, 11, 13, 17-20, 23-25, 27-32, 34-38, 40-46, 50-54, 56-64, and 66-73 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Granger *et al.* in view of various combinations of U.S. Patent No. 6,715,079 issued to Maytal (Maytal), U.S. Patent Application Publication No. 2002/0178412 in the name of Matsui (Matsui), U.S. Patent No. 6,598,162, issued to Moskowitz (Moskowitz), U.S. Patent No. 5,758,293, issued to Frasier (Frasier), U.S. Patent No. 5,892,899, issued to Aucsmith (Aucsmith), U.S. Patent No. 5,949,573, issued to Yarom (Yarom), U.S. Patent No. 5,850,554, issued to Carver (Carver), U.S. Patent No. 5,912,972, issued to Barton (Barton), and U.S. Patent No. 5,682,428, issued to Johnson (Johnson).

The arguments and remarks provided above with respect to rejections based on Granger *et al.* under 35 U.S.C. 102 also apply to the rejections of claims 5, 9, 10, 11, 13, 17-20, 23-25, 27-32, 34-38, 40-46, 50-54, 56-64, and 66-73 under 35 U.S.C. 103.

Because the arguments and remarks provided above with respect to rejections based on Granger *et al.*, under 35 U.S.C. 102 also apply to the rejections of claims 5, 9, 10, 11, 13, 17-20, 23-25, 27-32, 34-38, 40-46, 50-54, 56-64, and 66-73 under 35 U.S.C. 103, it is requested that the rejection of claims 5, 9, 10, 11, 13, 17-20, 23-25, 27-32, 34-38, 40-46, 50-54, 56-64, and 66-73 under 35 U.S.C. 103 be reconsidered and withdrawn.

Date: July 10, 2006



Joseph F. Oriti
Registration No. 47,835

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439